Piercing the Blockchain Veil: The Ontario Court’s Novel Pushback on Crypto Norwich Orders (Compared with the UK and DIFC)

June 22, 2026

Introduction: The Maturation of Crypto Asset Recovery

As digital asset markets expand, global courts are increasingly tasked with untangling complex, cross-border cryptocurrency disputes. When tokens are misappropriated, the immediate legal reflex for claimants is to pierce the pseudonymity of the blockchain. Universally, litigators have turned to the *Norwich Pharmacal* order (or *Bankers Trust* order), an equitable pre-action discovery tool used to compel innocent third parties, such as cryptocurrency exchanges, to disclose user identities and wallet transaction histories.

In recent years, jurisdictions like the United Kingdom (UK) and the Dubai International Financial Centre (DIFC) have adapted these common-law remedies to the speed of the digital era, granting disclosure orders against global exchanges to freeze and trace stolen crypto. However, a novel judgment from the Ontario Superior Court of Justice in May 2026, *Nivora Group LLC v. Ping et al., 2026 ONSC 2943*, signals a critical procedural divergence.

By refusing to grant a Norwich order against major crypto exchanges in a multi-million-dollar token dispute, the Ontario court has established a strict procedural boundary: the novel nature of cryptocurrency does not grant litigants reason to

bypass traditional rules of civil discovery.

The Ontario Approach: Striking a Balance Between Discovery and Privacy

The *Nivora* case involved a cross-border dispute over the creation and distribution of a "meme coin" known as TDCCP. The plaintiffs, corporate entities based in the UAE and the US, alleged that the Canadian developers of the token misappropriated over $6.2 million USD worth of Solana (SOL) and USDC, funneling the assets into wallets controlled by the defendants via the Kraken and VirgoCX exchanges.

To trace the ultimate destination of these funds, the plaintiffs sought a Norwich order compelling the exchanges to produce the wallet owners' identities and transaction records.

The Ontario Superior Court dismissed the motion, providing a rigorous check on the bounds of equitable relief. While the Court confirmed the modern reality that Norwich orders *can* legally be made against cryptocurrency exchanges (equating them to traditional financial institutions), it strictly applied the equitable test for necessity.

The novelty of the Ontario Court's decision lies in its refusal to treat a crypto dispute as inherently exempt from standard civil procedure. The Court denied the order on several key grounds:

1. **The "Known Defendant" Distinction:** In most crypto hacks, the perpetrators are anonymous "John Does," making an exchange the *only* practical source of information. In *Nivora*, the plaintiffs knew exactly who the defendants were, had already sued them, and the defendants were participating in the litigation.
2. **Circumvention of Standard Discovery:** The Court emphasized that a Norwich order is an "intrusive and extraordinary remedy," not a cost-saving shortcut. Because the plaintiffs could seek the same information

through standard pre-trial discovery (or via an Ontario Rule 30.10 motion for third-party production), the Norwich application was deemed an improper attempt to bypass the normal litigation regime.

3. **The *Mareva* Litmus Test:** A hallmark of urgent crypto tracing is the *ex parte* Norwich application paired with a *Mareva* (freezing) injunction to prevent the rapid dissipation of digital assets. The plaintiffs in *Nivora* waited months to bring the motion, brought it on notice to the defendants, and did not seek a freezing order. The Court noted that if the assets were truly at high risk of dissipation, they likely would have already vanished due to the delay. Thus, the privacy interests of unknown third-party wallet holders outweighed the plaintiffs' demand for immediate disclosure.

The UK Stance: The Proactive Standard for "Persons Unknown"

The Ontario ruling presents a stark contrast to the highly proactive stance of the English Commercial Courts. In the UK, judges view the speed and borderless nature of blockchain transactions as an existential threat to asset recovery.

While the UK courts apply a similar necessity test, their jurisprudence is heavily geared toward the "persons unknown" jurisdiction. English courts routinely issue *ex parte* Norwich Pharmacal and Bankers Trust orders against out-of-jurisdiction exchanges specifically to strip the pseudonymity of hackers. Recognizing the commercial reality of crypto tumbling and mixing, the UK courts frequently attach gagging orders to prevent platforms from tipping off the account holders, followed immediately by worldwide freezing injunctions.

The DIFC Perspective: Agility and the "Enforcement Principle"

Parallel to London, the DIFC Courts in Dubai have positioned themselves as a highly agile and pragmatic forum for digital asset tracing, applying English common-law principles through

the lens of regional commercial realities.

Supported by robust statutory frameworks, the DIFC Courts actively utilize injunctions and disclosure orders to prevent bad actors from moving assets beyond the reach of justice. The DIFC's willingness to support cross-border tracing is rooted deeply in its mandate to support international enforcement and prevent the thwarting of jurisdictional reach.

This is clearly illustrated in the recent DIFC Digital Economy Court judgment, *Techteryx Ltd v Aria Commodities DMCC [2025] DIFC DEC 001*. While assessing the continuation of sweeping proprietary and worldwide freezing injunctions (WFOs) involving hundreds of millions of dollars in allegedly misappropriated stablecoin reserves, H.E. Justice Michael Black KC emphasized the rationale for deploying such powerful interim remedies in aid of foreign proceedings:

"The object of the policy of the 'Enforcement Principle'… is to prevent the jurisdiction of the primary court from being thwarted… the Court must determine (1) whether there is a sufficient likelihood that a judgment enforceable through the process of the DIFC Courts will be obtained, and (2) a sufficient risk that without a freezing injunction execution of the judgment will be thwarted, to justify the grant of relief."

For the DIFC Courts, if a claimant can demonstrate a good arguable case of fraud and a real risk of dissipation, the court is highly likely to deploy its equitable arsenal, including WFOs and disclosure orders against digital asset platforms, to ensure that the ultimate judgment is not rendered hollow by the blockchain's speed. However, as the Ontario ruling cautions, these tools must be tethered to actual urgency and the prevention of thwarted jurisdiction, not abused as shortcuts to standard discovery.

Strategic Takeaways for Cross-Border Crypto Disputes

As global courts continue to adapt their traditional equitable frameworks to the cross-jurisdictional novelties of Web3 litigation, the contrast between the *Nivora* judgment and the approaches of courts in the UK and the DIFC provides a valuable strategic guide for managing international crypto disputes:

- **Sequencing Discovery Based on Defendant Identity:** The identity and litigation status of the alleged wrongdoer play a significant role in determining the appropriate discovery mechanism. In scenarios involving anonymous actors or "persons unknown," an equitable disclosure order against an exchange is often an essential tool for tracing. However, where defendants are known and actively participating in the litigation, parties must proactively assess whether standard civil discovery or conventional domestic third-party production rules should be pursued prior to seeking extraordinary equitable relief, as some forums will strictly require the exhaustion of these standard avenues first.

- **Synchronizing Interim Relief with Case Objectives:** Courts rigorously balance a claimant's need for information against the privacy rights of third-party account holders. When a disclosure application is based on the high risk of rapid crypto dissipation, parties should carefully align their procedural steps with that stated risk. Evaluating whether an *ex parte* application coupled with asset preservation measures, such as a worldwide freezing order (WFO) or *Mareva* injunction, is procedurally appropriate can help present a cohesive narrative of immediate urgency and necessity to the presiding adjudicator.

- **Navigating Forum-Specific Equitable Thresholds:** While blockchain technology is inherently borderless, the legal remedies to trace and recover digital assets remain distinctly territorial. The global landscape for

crypto asset tracing is not uniform; forums like the DIFC and the UK High Court have developed jurisprudence emphasizing the “Enforcement Principle” to facilitate rapid third-party disclosure and prevent the thwarting of jurisdictional enforcement. Conversely, other common-law jurisdictions may place equal or greater weight on the strict sequence of standard civil procedure and third-party privacy. Parties must map their asset recovery strategies to the specific evidentiary, equitable, and procedural thresholds of the chosen forum to optimize their prospect of recovery.

Wasel & Wasel advises on complex commercial disputes, international arbitration, and digital asset litigation. The firm possesses deep expertise in navigating cross-border fraud, tracing misappropriated funds, and securing interim equitable relief such as worldwide freezing injunctions and disclosure orders. By bridging the gap between local procedural frameworks and global common-law standards, Wasel & Wasel provides robust representation for corporate entities, tech developers, and international investors operating within the digital economy.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com